Remarks

Claims 1-19 and 21-23 are pending.

Applicant wishes to thank the Examiner for the courtesies extended during the Interview on September 11, 2006. During the Interview, the Applicant's representatives discussed several features of the invention, including the process used to register users with the document service cluster, and the aspects of the invention that allow the signing request to be generated at a remote computer in the absence of a pre-installed add-in software program configured for providing a signed message at the remote computer. Also during the Interview, Applicant's representatives discussed the fact that, in Applicant's invention, the private key portion remains on the document service cluster during the signing of the signature ready document, and no storage of the private key portion occurs on the remote computer after the signing of the signature ready document. At the end of the Interview, the Examiner suggested that the preamble of claim 1 be expanded to describe the computer environment in which the claimed method is implemented.

In an effort to advance the prosecution, all independent claims other than claim 1 have been cancelled. Applicant reserves the right to pursue the cancelled claims by way of one or more continuation applications. Applicant has amended independent claim 1 to include the features discussed during the Interview, and expanded the preamble as suggested by the Examiner.

As amended, claim 1 now recites a method for (i) issuing requests from remote computers to a document service cluster for signing electronic documents, and (ii) signing electronic documents using the document service cluster. The document service

cluster has a private key database, as well as secure access to a database of signature ready documents. The remote computers are coupled to the document service cluster over a computer network. In the claimed method, each of a plurality of users is registered using a registration process associated with the document service cluster. In the registration process: (i) each user provides identifying information corresponding to an identity of the user; (ii) a database check is performed of the identifying information provided by each user by comparing the identifying information provided by each user against database records; and (iii) each user is provided with service credentials for accessing the document service cluster if an outcome of the database check for the user is successful, whereby the user becomes a registered user.[1] Claim 1 also recites the step of securely storing a plurality of private key portions associated with the registered users in the private key database on the document service cluster.

Amended claim 1 also recites the step of receiving, at the document service cluster, a signing request and service credentials transmitted from a remote computer by a first registered user. The service credentials received at the document service cluster are used to identify the signing request as one transmitted by the first registered user. Significantly, the signing request is generated in the absence of a pre-installed add-in software program configured to providing a signed message at the remote computer. In

[1] Support for these registration steps may be found, for example, at page 20, lines 16 – page 21, line 19 of the Specification ("The invention allows people to register as users with the document service by presenting themselves at a registration center together with identification documents ... The person registering receives service credentials.... The service credentials can include access codes such as, for example, passwords ... that permit the user to access the user's service account from a user computer 104. ... Database checking can be used, for example, to detect people attempting [to] register as users under multiple identities by preventing multiple registration of the same ... identification documents.")

addition, the service credentials received from the first registered user are independent of the remote computer used to transmit the signing request to the document service cluster. Thus, in the present invention a user is permitted to sign a document from any remote computer that is connected to the network.[2] This aspect of Applicant's invention is clearly different from Bisbee, which limits the user to signing from a remote computer which has been configured with a special PCMCIA card for storage of private key information on the remote computer. *See* Bisbee, col. 3, lines 43-48 and col. 5, lines 1-12.

Claim 1 further recites the step of retrieving, from the private key database at the document service cluster, a private key portion associated with the first registered user. A complete private key is generated at the document service cluster using the retrieved private key portion if the retrieved private key portion is not a complete private key. A signature ready document is signed at the document service cluster using the complete private key to produce a signed document. Significantly, the private key portion remains on the document service cluster during the signing of the signature ready document, and no storage of the private key portion occurs on the remote computer after the signing of the signature ready document.[3] This aspect of Applicant's invention further differentiates

---

[2] Support for this aspect of the invention may be found, for example, at page 13, lines 10-12 of the Specification (A user is permitted "to sign a document from any user computer 104 that is connected to the web. No specialized software is required on the user computer 104 ...").

[3] Support for this limitation can be found, for example, at page 13, lines 13-14 of the Specification ("The user's private key and certificate remain securely on the document service cluster 102 at all times and are not stored on the user computer 104.")

Applicant's claims from Bisbee, which stores private key information on the remote computer using a PCMCIA card. *See* Bisbee, col. 3, lines 43-48 and col. 5, lines 1-12.

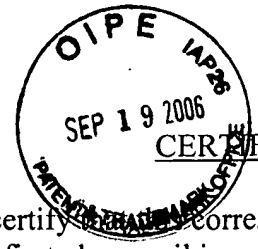
In view of the above, it is respectfully submitted that amended claim 1 is distinguishable from Bisbee, and in condition for allowance. It is also submitted that each dependent claim is allowable because it depends from an allowable base claim. A Notice of Allowance is therefore earnestly solicited.

The Commissioner is hereby authorized to charge any deficiency in the fees due in connection with this filing to Deposit Account 13-3403. A duplicate of this authorization is enclosed.

Dated: September 14, 2006

Respectfully submitted,

Stephen J. Stark
Miller & Martin PLLC
Suite 1000, Volunteer Building
832 Georgia Avenue
Chattanooga, Tennessee 37402-2289
423.756.6600



CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Commissioner for Patents
P. O. Box 1450
Alexandria, Virginia 22313-1450

on this 14th day of September 2006.

By: Beverly L. Middleton
Beverly L. Middleton